



Informational Notes for First Responders and Officials

Bulletin #46– March 8, 2004

www.sema.state.mo.us

Learning Management System Will Streamline SEMA's Training Program

The Learning Management System (LMS) will be replacing SEMA's current training scheduling system. According to SEMA's Training Officer, Jim Charrier, the new user friendly web based system should be on-line by mid-March. The system will allow each individual to set up personal account. Once logged into the system, individuals can enroll for SEMA training classes without reentering their personal information for each desired course, check on the status of enrollment, look up their course transcripts including independent study courses attended through EMI.

While the Learning Management System will make access and registration easier, SEMA will receive even greater benefit from the modernization of the system through better scheduling, financial tracking and the compilation of the EMI independent study and SEMA information.

Once the new system is up you may still access it through the SEMA website (www.sema.state.mo.us) by selecting the Training/Exercise/CERT choice on the SEMA homepage, just as in the past. Give it a try and let us know what you think.

Homeland Security Grant Gives Missouri Police Officers PPE

All Missouri commissioned police officers are being provided new personal protective safety equipment that would be needed if there were a biological, chemical threat or attack. SEMA purchased the equipment for all full-time police officers in Missouri with a Homeland Security grant. The Missouri Police Chiefs Association (MPCA) is distributing the equipment to all police departments.

Each kit consists of a gas mask, filters, Tychem suit, protective gloves, mask carrier bag and a gear bag. All police and law enforcement officers (including those who are currently overseas in the military) will receive their own kit after completing the training on how to use the equipment. The protective zip-up suit has a hood completely covers the police officer's body except for the face.

In addition to this safety equipment, a much higher level of suit is being provided to police officers who are members of the Missouri's 28 Homeland Security Response Teams. This equipment includes a breathing apparatus, so both police and firefighters can work a criminal scene. The police will be the ones to preserve the crime scene, and also help get people out following a biological, gas or chemical attack.

Missouri Fire Departments Receive Firefighter Grants

FEMA announced nine Missouri Fire Departments received Fire Grants in the final rounds 33 and 34. The grant for Fire Prevention went to: Sedalia FD (\$35,393). The grant for Fire Operation went to: Clinton FD (\$67,410); Grandview FD (\$74,673); Hannibal FD (\$50,220); Joplin FD (\$63,691); Marionville FD (\$29,238); Pattonville-Bridgeton Terrace FPD (\$109,695); Sikeston Dept of Public Safety (\$112,950); and St. Louis City FD (\$372,547).

In FY03, 266 Missouri Fire Departments received \$19,573,238 in Fire Grants from the Department of Homeland Security's FEMA and USFA.

Assistance to Firefighters Grant Program Application Period Opens

The Department of Homeland Security opened the application period for the Assistance to Firefighter

Grant Program on Monday, March 1, 2004 at and will be open through Friday, April 2, 2004. The Department invites fire departments throughout the United States to apply for assistance under this program.

The program assists rural, urban and suburban fire departments throughout the United States. These funds are used by the nation's firefighters to increase the effectiveness of firefighting operations, to improve firefighter health and safety programs and to establish or expand fire prevention and safety programs. Through the Department of Homeland Security Appropriations Act of 2004, Congress provided \$745.6 million for the Assistance to Firefighters Grant Program and transferred administration of the program from FEMA to ODP.

The FY 2004 AFGP closely mirrors previous years' programs with minor changes and enhancements. All the program areas and activities available last year are eligible for funding again this year. Emergency medical services activities, however, are not an independent program area for the 2004 program year. Rather, EMS activities have been incorporated into the appropriate activities under the Operations and Firefighter Safety Program. Additionally, this year all Federal grantees must obtain a DUNS number, (a unique nine-character identification number provided by the commercial company Dun & Bradstreet). The Federal government will use the DUNS number to better identify related organizations that are receiving funding under grants and cooperative agreements and to provide consistent name and address data for electronic grant applications.

Additional information about DUNS numbers can be found on the Dun & Bradstreet Web site (www.dnb.com/US/duns_update/index.html). There is no charge to obtain a DUNS number, and it is the applicant's responsibility to obtain one. It is recommended that applicants request a DUNS number as soon as possible by calling 1-800-333-0505.

As in past years, the Application and Program Guidance are automated and will be available online on March 1, 2004. They will both be accessible from the ODP Website (www.ojp.usdoj.gov/odp) and USFA Website (www.usfa.fema.gov <<http://www.usfa.fema.gov/>>). Additionally, the websites contain other useful background information on the AFGP, including a tutorial on applying for the program, a list of Frequently Asked Questions and the currently scheduled AFGP workshops.

Fire departments that have questions regarding the Assistance to Firefighters Grant Program should contact Bill Farr at the State Fire Marshall office (573) 751-2930 or contact the fire grant help desk at 1-866-274-0960 or at firegrants@dhs.gov.

DHS Approves National Incident Management System (NIMS)

U. S. Department of Homeland Security approved the National Incident Management System (NIMS), the Nation's first standardized management plan that creates a unified structure for Federal, state, and local lines of government for incident response. Response at real incidents now will be consistent. Key elements and features of NIMS include:

- * **Incident Command System (ICS).** Outlines a standard incident management organization called ICS that establishes five functional areas - command, operations, planning, logistics, and finance/administration - for management of all major incidents.

- * **Preparedness.** Responder readiness to manage and conduct incident actions is significantly enhanced if professionals have worked together before an incident. Preparedness also incorporates mitigation activities such as public education, enforcement of building standards and codes, and preventive measures to deter or lessen the loss of life or property.

- * **Communications and Information Management.** Standardized communications during an incident are essential. Interoperable communications systems are essential for incident and information management.

- * **Joint Information System (JIS).** Provides the public with timely and accurate incident information and unified public messages. This system employs Joint Information Centers and brings incident communicators together during an incident to develop, coordinate, and deliver a unified message.

- * **NIMS Integration Center (NIC).** The NIC will provide strategic direction and oversight of the NIMS, supporting both routine maintenance and continuous refinement of the system and its components over the long term.

NIMS is available at www.DHS.gov.

Protected Critical Infrastructure Information Sharing

DHS is launching the Protected Critical Infrastructure Information (PCII) Program. The PCII Program enables the private sector to voluntarily submit infrastructure information to the Federal government to assist the Nation in reducing its vulnerability to terrorist attacks. Critical infrastructure includes the assets and systems that, if disrupted, would threaten our national security, public health and safety, economy, and way of life. Although these industries, services and systems may be found in both the public and private sectors, the Department of Homeland Security estimates that more than 85 percent falls within the private sector.

Under provisions of the Critical Infrastructure Information Act of 2002 (CII Act), information that is voluntarily submitted per those provisions will be protected from public disclosure until and unless the PCII Program Office makes a determination that the information does not meet the requirements for PCII. If validated as PCII, the information will remain exempt from public disclosure. The rule establishing the procedures for PCII was published in the Federal Register. The PCII Program Office is part of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) Directorate and is charged with receiving submissions, determining if the information qualifies for protection and, if validated, sharing it with authorized entities for use as specified in the CII Act. For more information about the PCII Program, or to access the PCII regulation, please visit the PCII Program Office website on www.dhs.gov/pcii.

DHS Expands Information Exchange System to States and Major Cities

The Homeland Security Information Network initiative is expanding its computer-based counter-terrorism communications system to all 50 states, five territories, Washington, D.C., and 50 major urban areas to strengthen its flow of threat information. This communications capability will deliver to states and major urban areas real-time interactive connectivity with the Homeland Security Operations Center through the Joint Regional Information Exchange System (JRIES). This secure system will significantly strengthen the flow of real-time threat information at the Sensitive-but-Unclassified (SBU) level to all users immediately, and provides the platform for future classified SECRET communications to the state level. This collaborative communications environment, developed by state and local authorities, will allow all states and major urban areas to collect and disseminate information between federal, state, and local agencies involved in combating terrorism.

Standards Issued for Personal Protective Equipment

Homeland Security adopted standards regarding personal protective equipment developed to protect first responders against chemical, biological, radiological and nuclear incidents. These standards, which will assist state and local procurement officials and manufacturers, are intended to provide emergency personnel with the best available protective gear.

Homeland Security is adopting these standards, developed in partnership with the National Fire Protection Association (NFPA) and the National Institute for Occupational Safety and Health (NIOSH). These guidelines, which have also been adopted by the Interagency Board for Equipment Standardization and Interoperability, include NIOSH standards for CBRN three main categories of respiratory protection equipment and five current NFPA standards for protective suits and clothing to be used in responding to chemical, biological and radiological attacks. This provides the manufacturing community with minimum performance requirements for equipment, and the test methods to confirm that the required performance levels are achieved.

Pentagon Publishes Guide to Legal Authority of Emergency Responders

By Caitlin Harrington, CQ Staff

An Army task force has just arrived on the scene of what looks like a terrorist attack, a "dirty bomb" explosion. The FBI takes command and control of the scene. But it asks the Army's "Defense Coordination Element" to provide it with chemical and biological warfare experts.

The Army colonel in charge turns to his legal adviser in this hypothetical case: "Does the law," he asks, "allow the Defense Department to do this?" "Let's see," the lawyer might say, "on page 46 . . ." Far-fetched? Not anymore.

In recognition that all levels of emergency responders are likely to wrestle with questions about their authority in some large future terrorist incident, the Defense Threat Reduction Agency (DTRA) has published the first legal guidebook to deal with the issue.

The "Domestic WMD Incident Management Legal Desk book" is designed to provide the legal groundwork for federal and state lawyers and agency emergency planners in the throes of responding to a terrorist attack or natural disaster.

Legal Playbook: The handbook covers nearly every statute that could come into play during an emergency - from a description of laws on quarantining victims of chemical or biological attacks to a brief history of the Posse Comitatus Act (an 1878 law that generally bars the military from law enforcement activities) and a discussion of statutory exceptions to it.

The 529-page legal manual is probably the most comprehensive record of federal and state emergency laws to date. But as the emergency response "industry," grows, the guidebook will have to be updated to reflect changes in statutes and regulations. DTRA has tentative plans to periodically revise the handbook. A CD accompanies hard copies of the handbook, but the handbook is also available on the DTRA Web site at: <http://www.dtra.mil/news/deskbook/index.html>

DHS Issues First Radiological & Nuclear Detector Standards

The U.S. Department of Homeland Security's Science and Technology division today adopted its first radiological and nuclear detectors standards. The standards were developed in partnership with the Department's Office of Domestic Preparedness. These standards are designed to assist federal agencies, state and local officials, and manufacturers in procurement decisions related to radiological and nuclear detection equipment. These guidelines provide performance standards and test methods, as well as minimum characteristics for four classes of radiation detection equipment ranging from hand-held alarming detectors to radiation portal monitors for cargo containers. Officials receiving DHS grants through the Office of Domestic Preparedness will use these standards as technical guidance on performance specifications for detectors.

The Department of Commerce's National Institute of Standards and Technology, and the Department of Energy's National Laboratories (Pacific Northwest, Oak Ridge, Los Alamos and Lawrence Livermore) wrote the standards.

The four standards documents, which list performance specifications for radiation detectors, are available from IEEE (www.ieee.org) and from ANSI (webstore.ansi.org).